(54) Title: A DIGITAL SIGNATURE METHOD BASED ON BRAID GROUPS CONJUGACY AND VERIFY METHOD THEREOF

(54) 发明名称: 一种基于辫群共轭的数字签名及其验证方法
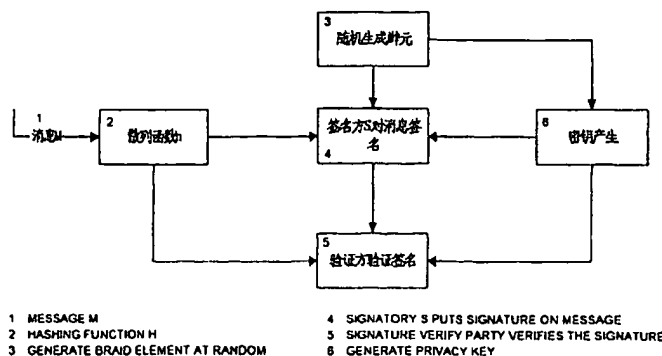
1 MESSAGE M	4 SIGNATORY S PUTS SIGNATURE ON MESSAGE
2 HASHING FUNCTION H	5 SIGNATURE VERIFY PARTY VERIFIES THE SIGNATURE
3 GENERATE BRAID ELEMENT AT RANDOM	6 GENERATE PRIVACY KEY

(57) Abstract: The present invention discloses a digital signature method based on braid groups conjugacy and a verify method thereof. The signatory S selects three braid elements that $x \in LB_m(1)$, $x' \in B_n(1)$, $a \in B_n(1)$, and considers the braid elements pair (x, x') to be the public key of the signatory S, braid element a to be the private key of the signatory S; signatory S obtains y ($y=h(M) \in B_n(1)$) using hashing function h; generate a braid element $b \in RB_{n-1-m}(1)$ at random, and then put signature on massage M to produce sign(M)= $a^{-1}byba^{-1}$ using its private key a an braid element b generated at random; signature verify party V acquires the public key of S, calculates message M using system parameter hashing function h, and gets y=h(M); determine whether sign(M) and M are conjugate or not, if yes, calculate sign(M)x' and xy using the public key of S which is obtained already and determine whether they're conjugate; if not, sign(M) is the invalid, that's to say, verify fails; if yes, sign(M) is the valid signature for message M. The present invention avoids k-CSP problem in SCSS signature scheme of prior art, increasing the safe degree of signature algorithm, decreasing the number of braid elements used and the times of conjugacy determination in order to improve the calculating efficiency of signature greatly, without reducing the safety.

(57) 摘要

本发明公开了一种基于辫群共轭的数字签名及其验证方法，签名方S选择三个辫元$x \in LB_m(l)$，$x' \in B_n(l)$，$a \in B_n(l)$，将辫元对(x', x)作为签名方S的公钥，辫元a作为签名方S的私钥；签名方S使用散列函数h得到$y=h(M) \in B_n(l)$；随机生成一个辫元$b \in RB_{n-1-m}(l)$，然后使用自己的私钥a和产生的随机辫元b对消息M签名得到$Sign(M) = a^{-1}byb^{-1}a$；签名验证方V获取S的公钥，利用系统参数散列函数$h$对消息M进行计算，得到$y=h(M)$；判定$sign(M)$与$y$是否共轭，若共轭，利用已获取的S的公钥计算$sign(M) x'$和$xy$，并判定二者是否共轭，若不共轭，则$sign(M)$不是一个合法签名，验证失败；若共轭，则$sign(M)$为消息M的合法签名。本发明避免了现有技术中SCSS签名体制中的k-CSP问题，提高了签名算法的安全性，在不降低安全性的基础上，减少了参与的辫元的数目和共轭判定的次数，从而大大提高了签名的运算效率。